OMNIKEY®8751 e-Health LAN

eHealth-BCS Terminal

BEDIENUNGSANLEITUNG

Stand: 13. Januar 2009
Dokument Nummer 8751-901, Rev A.123

This product includes software developed by Go Ahead Software, Inc. Copyright (c) 2008 GoAhead Software, Inc. All Rights Reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/). This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

This product includes software developed by the University of California, Berkeley and its contributors.

Bei der mitgelieferten PC-Software zur Nutzung des eHealth Terminals OMNIKEY 8751 e-Health LAN handelt es sich um proprietäre Software von OMNIKEY, für die die OMNIKEY Enduser-Lizenz (OMNIKEY Enduser-License-Agreement EULA) gilt.

Teile der im Gerät verwendeten Software-Pakete sind Open Source Software und werden verwendet und lizenziert unter den Bestimmungen der jeweils geltenden Lizenzbestimmungen.

Der volle Wortlaut der Lizenztexte befindet sich sowohl auf der dem Gerät beiliegenden CD-Rom als auch in dem beiliegenden Lizenzheft.

© 2008 OMNIKEY GmbH. All rights reserved. Alle Rechte vorbehalten.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

Inhaltsverzeichnis

Überblick **6**
Einführung 6
Produkt 6
Support 6

1 Sicherheitshinweise **7**
1.1 Allgemeines 7
1.2 Siegelung 8
1.3 Fehlermeldungen 9

2 Lieferumfang **10**

3 Hardware **11**

4 Geräte-Elemente **12**
4.1 Gerätevorderseite 12
4.2 Geräterückseite 13
4.3 Heilberufsausweis Auswurfsicherung 13
4.4 Anzeige-Elemente 14

5 Kartenschnittstellen **15**
5.1 Schnittstellen für kontaktbehaftete Smart Cards 15
5.2 Kontaktlose Schnittstelle 16

6 Geräte-Menü **17**
6.1 Funktions-Übersicht Menü 17
6.2 Verwendung der Tastatur 18
6.3 Änderung der Baudrate 18
6.4 Änderung der Geräte-PIN 18

7 Inbetriebnahme **19**
7.1 Standort 19
7.2 Stromnetz 19
7.3 Geräte-PIN (Transport-PIN) 19
7.4 Serielle Schnittstelle 20
7.5 Netzwerk 20
7.5.1 Kabelverbindungen 21
7.5.2 Anschluss eines weiteren Netzwerkgerätes 21
7.5.3 Automatische Netzwerk-Konfiguration via DHCP 21
7.5.4 Überprüfung der DHCP Konfiguration 21
7.5.5 Konfiguration ohne DHCP Server 22

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

8 Webschnittstelle 23
8.1 Allgemeines 23
8.2 Browser Warnmeldung (Zertifikatefehler) 24
8.3 Authentizitätsprüfung der Webschnittstelle 24
8.4 Login 25
8.5 Status Anzeige und Warmstart 26
8.6 IP Konfiguration 27
8.7 Functional Units 28
8.8 Firmware Upload 29
8.9 Passwörter ändern 30

9 Hardware-Reset 31

10 Upgrade von Firmware 32
10.1 Allgemeines 32
10.2 Quelle für neue Firmware 32
10.3 Sicherheitshinweise 32
10.4 Durchführung des Updates 34

11 BCS Funktion 36
11.1 Direkte Verwendung der seriellen Schnittstelle 36
11.2 Verwendung der CT-API 36
11.2.1 Verwendung der CT-API über die serielle Schnittstelle 36
11.2.2 Verwendung der CT-API über das LAN (CT-API LAN Tunnel) 36
11.3 Mehrbenutzerbetrieb im LAN 37
11.4 Dualbetrieb Seriell und LAN 37

12 SICCT Funktion 38
12.1 Service Discovery 38
12.2 Kommando-Interpreter 38

13 Konformitätserklärung 39

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

Abbildungsverzeichnis

Abbildung 1: Sicherheitssiegel 7
Abbildung 2: Gerätesiegel 8
Abbildung 3: Position der SIM-Karten Steckplätze 8
Abbildung 4: Geräte-Elemente vorne 12
Abbildung 5: Geräte-Elemente hinten 13
Abbildung 6: Entfernen des Auswerfers (links) und gesicherter Auswerfer (rechts) 13
Abbildung 7: LED Anzeige (schematische Darstellung) 14
Abbildung 8: Steckrichtung eGK / KVK Karte 15
Abbildung 9: Steckrichtung HBA 15
Abbildung 10: SMC Karten Steckrichtung (links) und voll eingesetzt (rechts) 16
Abbildung 11: RFID Schnittstelle 16
Abbildung 12: Terminal Tastatur 18
Abbildung 13: Anschlüsse Geräterückseite und grüner LAN Stecker 20
Abbildung 14: Zertifikate-Warnmeldung der Webschnittstelle (IE 7 und Firefox) 24
Abbildung 15: Webschnittstelle Login 25
Abbildung 16: Status und Neustart Button 26
Abbildung 17: Konfigurationsmenü 27
Abbildung 18: Functional Units 28
Abbildung 19: Reiter Firmware Upload 29
Abbildung 20: Benutzerpasswörter ändern 30
Abbildung 21: Firmware Upload 34
Abbildung 22: Neustart-Seite 35

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

Überblick

Einführung

Bitte lesen Sie vor Inbetriebnahme des Geräts diese Anleitung vollständig durch, insbesondere den Abschnitt 1: Sicherheitshinweise

Warnung:
Aus sicherheitstechnischen Gründen können weder *geänderte Passwörter* noch die *Geräte-PIN* wiederhergestellt oder zurückgesetzt werden.

Verlorene *Geräte-PIN oder Passwörter* können das Gerät dauerhaft unbrauchbar machen.

Produkt

Diese Betriebsanleitung beschreibt die Nutzung des eHealth-BCS Terminals

OMNIKEY 8751 e-Health LAN

Das Gerät entspricht den aktuellen Vorgaben der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) zum Einsatz von eHealth-BCS Terminals im Rahmen der Telematik-Infrastruktur der elektronischen Gesundheitskarte (eGK) in Deutschland.

Das Gerät ist für den Einsatz als eHealth Terminal vorbereitet und erfüllt alle Voraussetzungen für den späteren Einsatz als Signaturterminal im Deutschen Gesundheitswesen in Übereinstimmung mit den Sicherheitsanforderungen der Verordnung zur elektronischen Signatur (SigV) §15 Absatz 2 und 4 und dem Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG) §17 Absatz 2. Die Funktionalität wird durch Firmware-Upgrade erreicht. Die Bedienungsanleitung für den Einsatz als Signaturterminal muss zum entsprechenden Zeitpunkt von den Internetseiten des Herstellers herunter geladen werden.

Support

OMNIKEY Support
OMNIKEY GmbH
Fax: +49 6123 791328
Email: support@omnikey.com

Produkt-Website
http://www.hidglobal.com/8751de

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

1 Sicherheitshinweise

1.1 Allgemeines

Bei der Benutzung des Gerätes beachten Sie bitte die folgenden generellen Sicherheitshinweise:

- Das Gerät muss vor der Aktivierung und ersten Verwendung eindeutig als Originalgerät des Herstellers identifiziert werden. Dazu muss sich der Anwender von der Unversehrtheit der Verpackung, des Gerätes selbst und dessen Versiegelung überzeugen. Nur so ist sichergestellt, dass ein authentisches Gerät des Herstellers in Betrieb gesetzt wird.
- Das Gerät darf ohne zusätzliche organisatorische Maßnahmen nur in einer kontrollierten Einsatzumgebung verwendet werden.
- Der Einsatz in einer nicht überwachten Einsatzumgebung ist nur zulässig, wenn das Gerät nicht länger als eine halbe Stunde unbeaufsichtigt betrieben wird. Andererseits ist der Betrieb in einer nicht überwachten Einsatzumgebung nur zulässig, wenn folgende organisatorische Maßnahmen gewährleistet sind:
  - (A) Das Gerät wird nur im Dauerbetrieb in einer Anwendung eingesetzt
  - (B) Der Host, als steuernde Instanz innerhalb der Anwendung, überprüft die Anwesenheit des Gerätes mindestens 1-mal pro halbe Stunde.
- Beide grauen, mit einem Hologramm und dem OMNIKEY Schriftzug versehenen Sicherheitssiegel (Abbildung 1) müssen unversehrt sein. Dies stellt sicher, dass das Gerät ungeöffnet ist und somit nicht manipuliert wurde. Bitte überprüfen Sie auch die Identität des Holgramms.

1 = OMNIKEY Schriftzug
2 = Hologramm
3 = graues Siegelmaterial

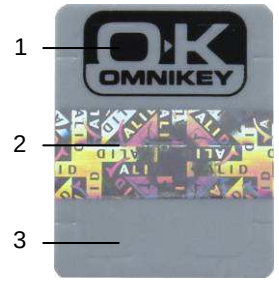

Abbildung 1: Sicherheitssiegel

- Die Sicherheitssiegel des Gerätes befinden sich auf der Vorder- und Oberkante im sichtbaren Bereich und sind über die Trennkante der Gehäuseschalen geklebt (Abbildung 2). Die Unversehrtheit der Siegel ist vor jeder Benutzung des Gerätes zu überprüfen.
- Beim Einschalten des Gerätes und während des Betriebes können Sicherheitshinweise auf dem Display angezeigt werden. Meldet das Gerät eine Sicherheitswarnung, ist es nicht mehr betriebsbereit. Es ist nach den Erläuterungen in Kapitel 1.3 Fehlermeldungen zu verfahren.
- Der Administrator und der medizinische Leistungserbringer sind für die sichere Handhabung des Gerätes verantwortlich. Insbesondere muss sich der Betreiber des Gerätes mit den Sicherheitsvorkehrungen, die zum Schutz des Gerätes notwendig sind, vertraut machen.
- Das Gerät verfügt über eine Geräte-PIN zum Freischalten sicherheitsrelevanter Aktivitäten und zum Öffnen sicherheitsrelevanter Dialoge über das Tastenfeld. Die Geräte-PIN muss bei der ersten Inbetriebnahme von der Transport-PIN in eine individuelle 6-stellige PIN geändert werden. Benutzen Sie keine Jahrestage oder fortlaufende Ziffernfolgen. Die Geräte-PIN ist durch den Betreiber geheim zu halten.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

1.2 Siegelung

Bitte prüfen Sie vor jeder Benutzung die Siegel des Gehäuses auf Unversehrtheit.

Abbildung 2: Gerätesiegel

Für den Betrieb des Gerätes als Signaturterminal in einer Signaturanwendungskomponente sind so genannte Sicherheitsmodule (SM-KT, SMC-A oder SMC-B) erforderlich. Die Sicherheitsmodule sind als Smart Card im Formfaktor ID-000 (SIM Format) ausgeprägt und gehören nicht zum Lieferumfang des Gerätes. Sie werden vom Betreiber an der Seite des Gerätes eingesetzt und ebenfalls versiegelt. Zu diesem Zweck befinden sich zwei Steckplätze für Smart Cards im SIM Format an der rechten Seite des Gerätes im sichtbaren Bereich (Abbildung 3). Auch diese Siegel sind vor jeder Benutzung auf Unversehrtheit zu überprüfen.

Abbildung 3: Position der SIM-Karten Steckplätze

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

1.3 Fehlermeldungen

Das Gerät verfügt über Sicherheitsmechanismen zum Schutz vor Manipulation im nicht sichtbaren Bereich. Bei Anzeige einer der folgenden Warnungen ist das Gerät nicht mehr betriebsbereit. Bei entsprechenden Warnungen gehen Sie bitte wie beschrieben vor:

Meldung: „Manipulation erkannt >Sicherheitsprüfung<"

Das Gerät ist bei Anzeige dieser Meldung nicht mehr verwendbar. Bitte senden Sie das Gerät zur Überprüfung an einen autorisierten Fachhändler. Besteht Verdacht auf Manipulation, darf das Gerät nicht wieder in Betrieb gesetzt werden und ist einer fachgerechten Entsorgung zuzuführen.

Meldung: „Unterspannung!!! >Gerät überprüfen<"

Das Gerät war für längere Zeit vom Stromnetz getrennt (länger als 4 Wochen). Das Gerät muss vor der erneuten Aktivierung nochmals eindeutig als Originalgerät des Herstellers identifiziert werden, so wie bei der Erstinbetriebnahme. Dazu muss sich der Anwender von der Unversehrtheit des Gerätes und der Versiegelung überzeugen. Zur erneuten Inbetriebnahme ist die Eingabe der Geräte-PIN zwingend erforderlich. Das Gerät meldet sich dann mit:

„Unterspannungswarnung behoben!"

Bitte beachten Sie, dass dieses Verhalten notwendig ist, um die Gerätesicherheit zu garantieren. Andernfalls würde ein kostenpflichtiger Servicefall generiert.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

2 Lieferumfang

Bitte prüfen Sie nach Erhalt den vollständigen Lieferumfang ihres OMNIKEY® 8751 e-Health LAN Lesers:

- OMNIKEY® 8751 e-Health LAN
- Netzwerkkabel (8-adrig, CAT 5 UTP LAN Patch Kabel RJ-45)
- Externes AC/DC Steckernetzteil (Input 100-240 V, 0.3A , 50-60 Hz, Output +5V, 2A max.)
- Serielles Anschlusskabel für BCS Funktion (4-adrig, 9-Pol. SUB Stecker auf RJ-11m)
- Bedienungsanleitung
- Lizenzheft
- CD-ROM
- Grüner Schutzstecker für die Netzwerkbuchse (LAN) am Gerät

Bitte kontaktieren Sie Ihren Fachhändler, wenn der Lieferumfang nicht vollständig ist.

Bitte bewahren Sie die Lieferverpackung des Gerätes auf, um den Leser im Falle eines Defektes sicher einsenden zu können.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

3 Hardware

Das Terminal verfügt über folgende Hardware-Merkmale:

- Farbe: weiß / transparent
- Maße (LxBxH): 220x160x90 mm
- Gewicht: ca. 1210 gr, mit Netzteil ca. 1350 gr
- Betriebstemperatur: 0 - 55 Grad Celsius
- Feuchtigkeit: 10-90% rH (nicht kondensierend)
- 1 x LAN Anschluss (Fast Ethernet RJ-45 Netzwerk, 10/100 Mbit/s auto-sensing)

  (Zweiter LAN Anschluss unter Verwendung eines Portdopplers für strukturierte Ethernet-Verkabelung / Portdoppler nicht im Lieferumfang enthalten)
- 1 x Serieller Anschluss (RJ-11)
- LED Statusanzeige
- Zweizeiliges Display
- Tastatur mit 25 Tasten

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

4 Geräte-Elemente

4.1 Gerätevorderseite

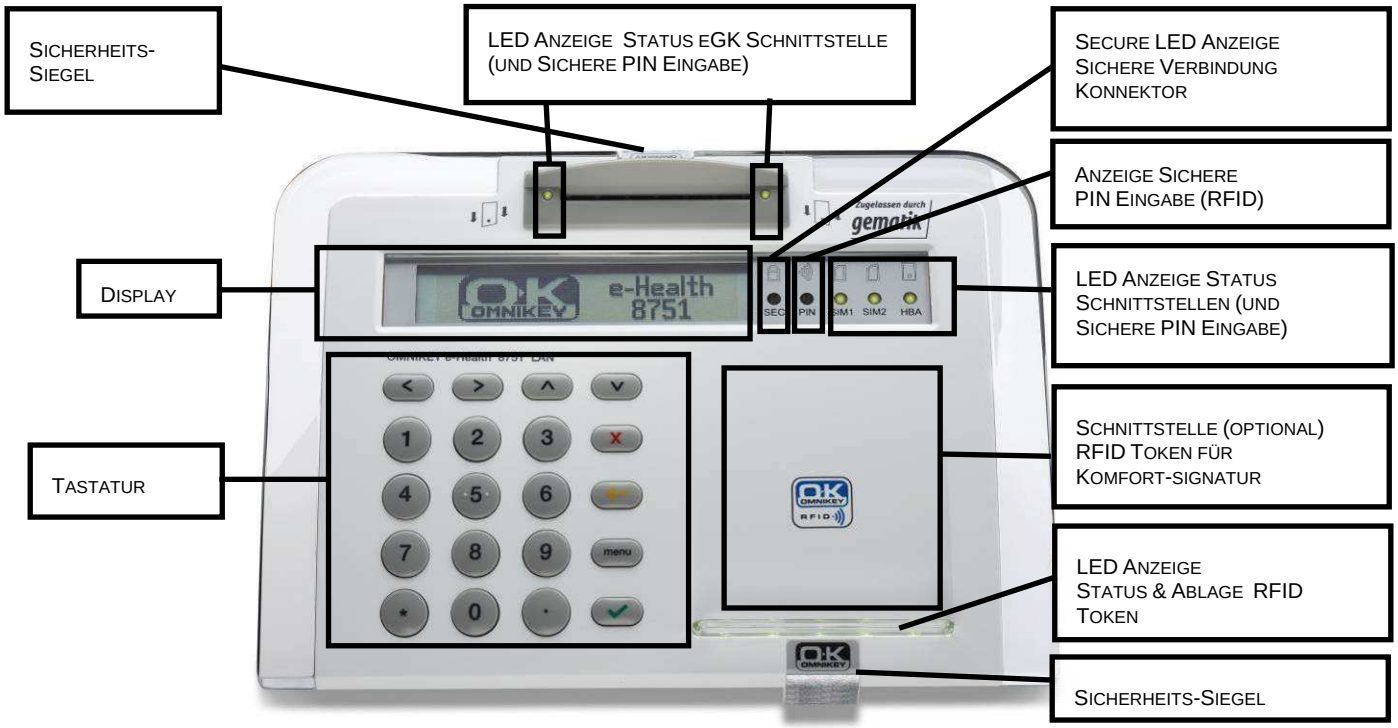

Abbildung 4: Geräte-Elemente vorne

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

4.2 Geräterückseite

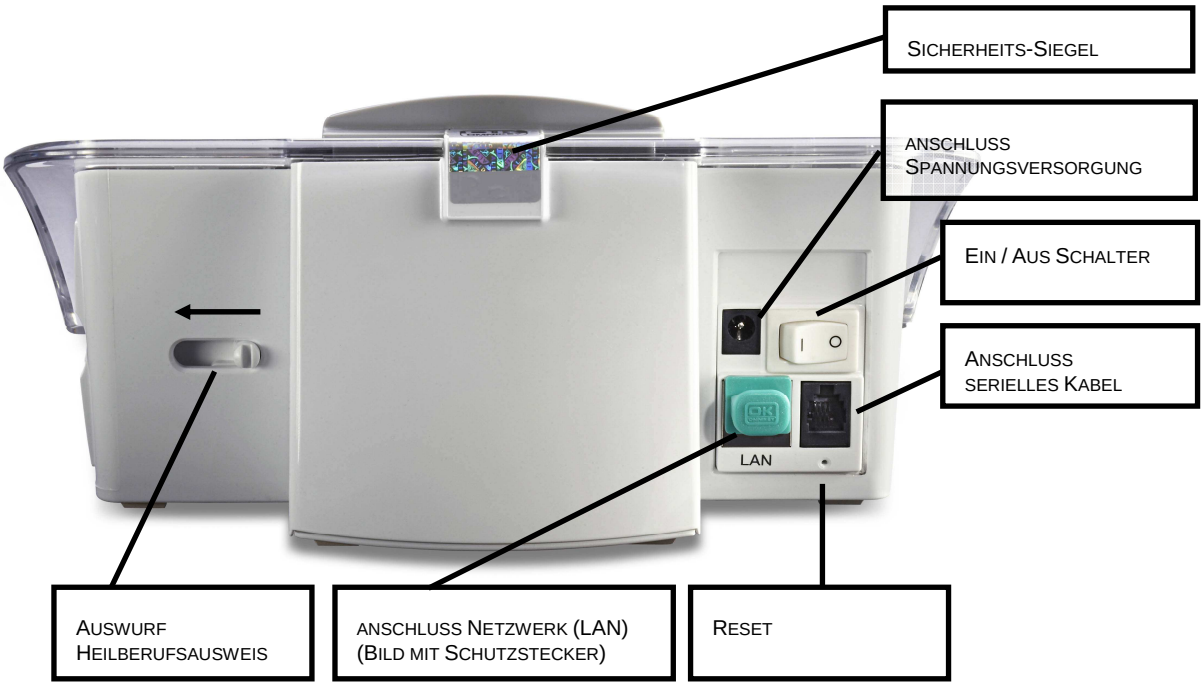

Abbildung 5: Geräte-Elemente hinten

4.3 Heilberufsausweis Auswurfsicherung

Zur Sicherung des Heilberufsausweises (HBA) vor unbefugter Entnahme kann der Auswerfer-Stift auf der Gehäuserückseite entfernt werden.

Abbildung 6: Entfernen des Auswerfers (links) und gesicherter Auswerfer (rechts)

Zum Entfernen des Auswerfer-Stiftes drehen Sie bitte den Stift an der Kerbe mit einem Schraubendreher gegen den Uhrzeigersinn vorsichtig um 90 Grad (s. Bild oben links) und ziehen ihn dann nach hinten weg. Wollen Sie den Stift wieder einsetzen, verfahren Sie bitte in umgekehrter Reihenfolge.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

4.4 Anzeige-Elemente

Das Terminal verfügt über mehrere LEDs, die grün und / oder rot leuchten.

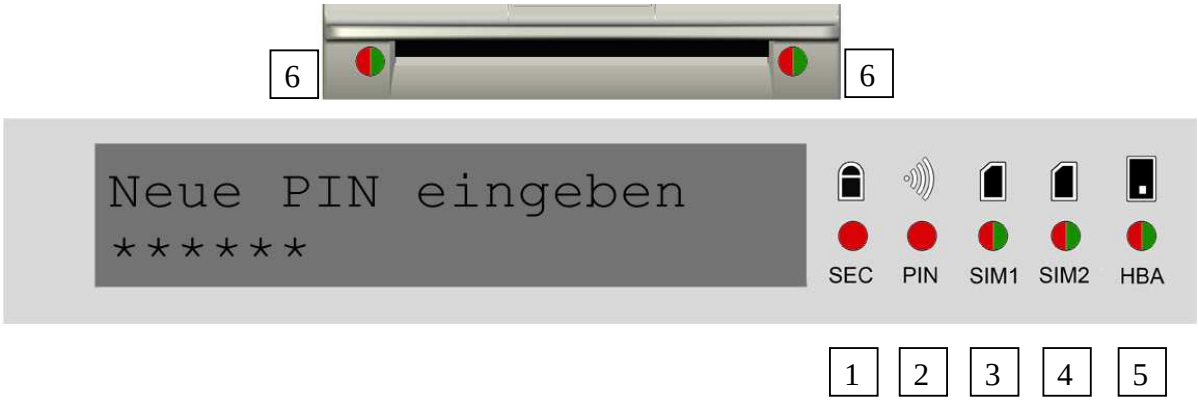

Abbildung 7: LED Anzeige (schematische Darstellung)

Die LEDs informieren den Anwender über folgende wichtigen Gerätezustände:

LED Position	Bedeutung	LED		Farbe	Erklärung
1	SEC	1		Rot	Sicherer Zustand des EVG
2	PIN RFID	2		Rot blinkend	Sichere RFID Kommunikation
3	SIM1	3		Grün	Betriebsbereit
				Grün blinkend	ICC Kommunikation
		4		Rot blinkend	sichere PIN-Eingabe
4	SIM2	5		Grün	Betriebsbereit
				Grün blinkend	ICC Kommunikation
		6		Rot blinkend	sichere PIN-Eingabe
5	HBA	7		Grün	Betriebsbereit
				Grün blinkend	ICC Kommunikation
		8		Rot blinkend	sichere PIN-Eingabe
6	eGK / KVK	9	11	Grün	Betriebsbereit
				Grün blinkend	ICC Kommunikation
		10	12	rot blinkend	sichere PIN-Eingabe

Im BCS Betrieb ist nur die grünen LED (Position 6) der KVK (Betriebsbereit / ICC Kommunikation) von Bedeutung.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

5 Kartenschnittstellen

5.1 Schnittstellen für kontaktbehaftete Smart Cards

Das Kartenterminal verfügt über folgende Kartenschnittstellen:

- Steckplatz für elektronische Gesundheitskarte (eGK): 1 x ID-1 (Volle Kartengröße) Einschub der Karten erfolgt von oben mit Chip nach unten & vorne bis zum Einrasten. Vollständig gesteckt ragt die Karte noch zu ca. einem Drittel aus dem Steckplatz. Auswurf der Karte erfolgt durch einfaches Herausziehen der Karte.

- Steckplatz für Heilberufsausweis (HBA): 1 x ID-1 (Volle Kartengröße) Einschub der Karten erfolgt von rechts mit Chip nach links & vorne). Die Karte wird durch Betätigung des HBA Auswerfers im Einschub **vollständig** versenkt. Auswurf der Karte erfolgt durch Schieben des HBA Auswerfers auf der Gehäuse-Rückseite in Pfeilrichtung (s. Abbildung 5: Geräte-Elemente hinten). Lässt sich die Karte nicht vollständig in den Einschub versenken, prüfen und ändern Sie bitte die Position des HBA Auswerfers auf der Gehäuse-Rückseite so wie abgebildet (s. Abbildung 5: Geräte-Elemente hinten)

Abbildung 8: Steckrichtung eGK / KVK Karte

Abbildung 9: Steckrichtung HBA

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

- Secure Module Slots: 2x ID-000 (SIM-Kartengröße)
  Einschub der Karte erfolgt jeweils mit dem Chip zur Gehäuserückseite und Karten-Schräge nach unten zeigend bis zum Einrasten.
  Auswurf der Karte erfolgt durch Eindrücken der Karte in den Slot zum Auslösen der Push-Push-Mechanik, welche die Karte auswirft.

Abbildung 10: SMC Karten Steckrichtung (links) und voll eingesetzt (rechts)

5.2 Kontaktlose Schnittstelle

Neben den Schnittstellen für kontaktbehaftete Smart Cards ist das Terminal bereits mit einer RFID (Radio Frequency Identification Device) Schnittstelle für kontaktlose Smart Cards bzw. sogenannter RFID Tokens vobereitet.

Abbildung 11: RFID Schnittstelle

Diese Schnittstelle kann für später Anwendungen wie z.B. der Komfort-Signatur oder andere RFID Anwendungen im Rahmen ihres Praxis-Software freigeschaltet werden. Diese Freischaltung ist u.U. kostenpflichtig.

Zur Verwendung halten Sie die kontaktlose Smart Card (oder Token) in ca. 1 - 2 cm Abstand direkt vor das OMNIKEY RFID Logo, oder platzieren Sie die Karte auf der Ablage unter dem Logo.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

6 Geräte-Menü

6.1 Funktions-Übersicht Menü

Am Geräte Menü können folgende Einstellungen vorgenommen werden:

- Änderung der Baud Rate für die serielle Schnittstelle
- Änderung der Geräte PIN

Des weitern können folgende Informationen zum Gerät abgerufen werden:

- IP Adresse mit Subnetz Maske
- Mac Adresse
- Firmware Version

Die folgende Tabelle erhält eine Übersicht über die genannten Menüfunktionen sowie die zum Aufrufen notwendigen Tastenfolgen.

1. Taste	2. Taste	3. Taste	Anzeige auf Display	Hinweis
(menu)	(1) Status	(1) IP	Anzeige von IP Adresse und Subnetz Maske	n/a = NOT AVAILABLE (Das Gerät hat keine gültige IP Adresse)
		(2) Mac	Anzeige von MAC Adresse	Benötigt zur Konfiguration des CT-API LAN Tunnels
		(3) FW Version	Anzeige von FW Version	Benötigt im Support Fall
	(2) Einstellungen	(1) COM	Baud (1) 9600 (2) 115200	Stern markiert aktiven Wert. Default 9600
		(2) PIN	Ändern der Geräte PIN	Aktuelle PIN eingeben, dann neue PIN eingeben **Achtung: eine verlorene Geräte-PIN kann das Gerät dauerhaft unbrauchbar machen.**

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

6.2 Verwendung der Tastatur

Die Tastatur wird zur Steuerung der Menüfuktionen, der PIN Eingabe sowie der Displaysteuerung verwendet.

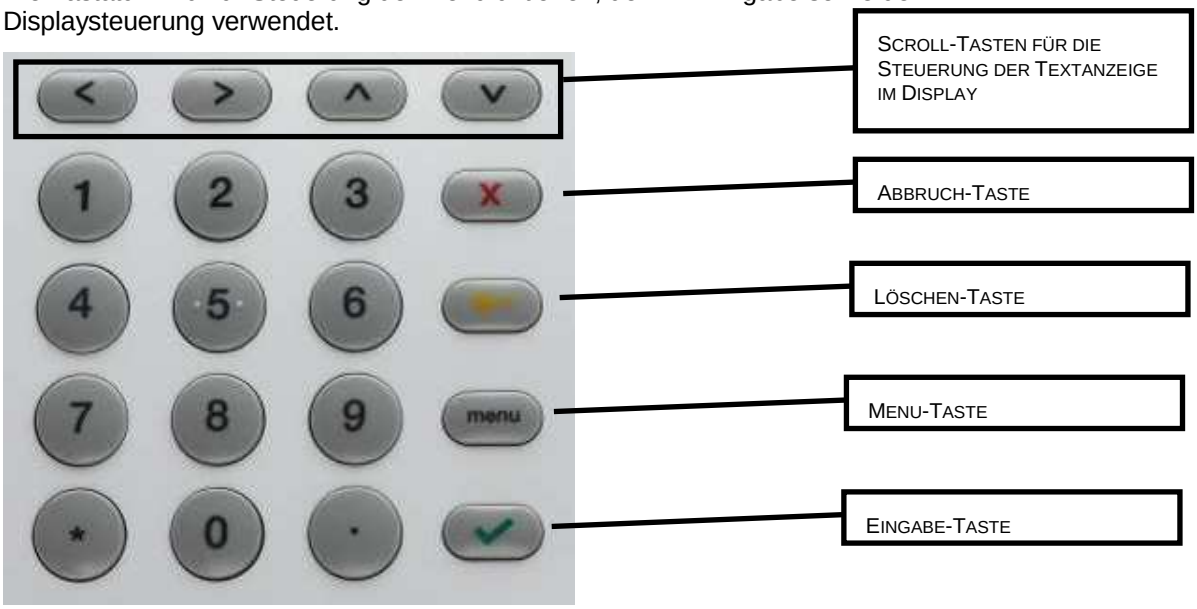

Abbildung 12: Terminal Tastatur

-> Eingaben (z.B. von PIN Nummern) müssen mit der Eingabe-Taste bestätigt werden.

6.3 Änderung der Baudrate

Zum Ändern der Baud Rate des Terminals drücken Sie:

menu -> (2) Einstellungen -> (1) COM

Im Auslieferungszustand ist das Gerät auf 9600 Baud eingestellt. Auf dem Display steht:

Meldung: **„(*) 9600 (2) 115200“**

Durch Drücken der Taste (2) stellen Sie das Gerät dauerhaft auf 115200 Baud um.

6.4 Änderung der Geräte-PIN

Achtung: eine verlorene Geräte-PIN kann das Gerät dauerhaft unbrauchbar machen.

Zum Ändern der Geräte PIN (manchmal auch als Direkt PIN bezeichnet) drücken Sie:

menu -> (2) Einstellungen -> (1) PIN

Es erfolgt ein Quittungston.

Meldung: **„PIN Eingeben“**

Eingabe (der Transport PIN im Auslieferungszustand): **„123456“**

Meldung: **„Neue PIN eingeben“**

Eingabe der neuen PIN (mindestens sechs Stellen).

Meldung: **„Neue PIN wiederholen“**

Eingabe der neuen PIN.

Meldung: **„PIN Änderung erfolgreich!“**

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

7 Inbetriebnahme

Lesen Sie bitte vor der Inbetriebnahme Kapitel 1 Sicherheitshinweise.

7.1 Standort

Prüfen Sie vor der Inbetriebnahme den sicheren und festen Stand des Gerätes, sowie eine ausreichende Nähe zur nächsten Steckdose und ggf. zur seriellen Schnittstelle des Rechners oder zum LAN Anschluss.

7.2 Stromnetz

Mit Anschluss an das Stromnetz und Betätigung des Schalters auf der Rückseite wird das Gerät aktiviert und ein Selbsttest gestartet, der folgende Phasen durchläuft:

- Geräteaktivierung und kurzer Quittungston (Beep)
- Aktivierung der LEDs
- Aktivierung des Displays mit OMNIKEY Schriftzug
- Doppelter Quittungston (Beep – Beep)

Mit dem doppelten Quittungston ist das Gerät betriebsbereit. Der Selbsttest dauert ca. 20 Sekunden.

7.3 Geräte-PIN (Transport-PIN)

Beim ersten Start des Gerätes (oder auch beim Einspielen einer neuen FW) wird das Terminal die Geräte-PIN abfragen. Beim ersten Start muss die Transport-PIN in eine 6-stellige individuelle Geräte-PIN geändert werden. Beachten Sie bitte die Sicherheitshinweise in Kapitel 1 zum Umgang mit der Geräte-PIN.

Die Standard Transport-PIN im Auslieferungszustand ist: „123456“

Die Eingabe der Geräte-PIN ist zum Freischalten sicherheitsrelevanter Aktivitäten (z.B. ein Firmware-Update) und zum Öffnen sicherheitsrelevanter Dialoge erforderlich und muss direkt am Tastenfeld des Gerät eingeben werden.

Gehen Sie mit der Geräte-PIN so sorgfältig um, wie mit Ihrer persönliche Signatur-PIN. Nur so kann der sichere Betrieb gewährleistet werden. Benutzen Sie keine Jahrestage, Geburtstage oder fortlaufenden Ziffernfolgen.

→ Aus Sicherheitsgründen ist die Geräte-PIN nicht rücksetzbar. Bei Verlust der Geräte-PIN ist das Gerät für den späteren Einsatz als Signaturterminal im Deutschen Gesundheitswesen nicht mehr brauchbar und muss ggf. ausgetauscht werden.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

7.4 Serielle Schnittstelle

Der Anschluss der seriellen Schnittstelle befindet sich auf der Geräte-Rückseite rechts unter dem Ein / Aus Schalter. Bitte verbinden sie das mitgelieferte (vieradrige) serielle Kabel mit dem Terminal und dem PC.

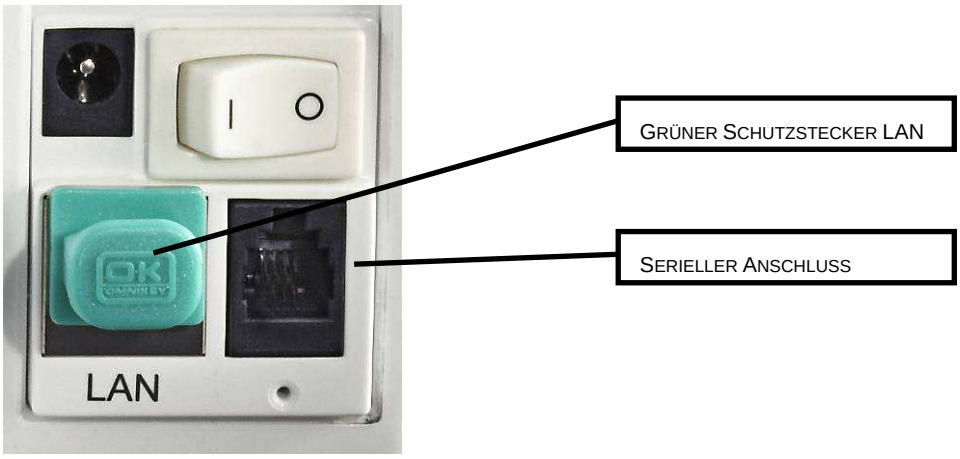

Abbildung 13: Anschlüsse Geräterückseite und grüner LAN Stecker

-> Im Auslieferungszustand ist der Netzwerkanschluss (LAN) mit einem grünen Stecker versehen. Dieser Stecker dient zum Schutz des Anschlusses sowie zum vermeiden von Verwechslungen. Sofern sie nicht den Netzwerkanschluss verwenden, lassen sie den Stecker bitte auf der LAN Buchse.

7.5 Netzwerk

Der Stecker zum Anschluss des Netzwerkes befindet sich an der Gehäuserückseite (s. Abbildung 13: Anschlüsse Geräterückseite und grüner LAN Stecker). Bitte beachten Sie, dass ein Anschluss an ein Netzwerk nur dann erforderlich ist, wenn das Gerät über das LAN betrieben werden soll. Bitte entfernen Sie zum Betrieb in einem LAN den grünen Schutzstecker von der LAN Buchse.

Der OMNIKEY® 8751 e-Health LAN ist zur Verwendung in TCP/IP-basierenden lokalen Netzwerken (Local Area Network - LAN) ausgelegt. Zur einfachen und schnellen Inbetriebnahme wird ein entsprechender **LAN Anschluss** und ein **DHCP Server** benötigt. Für Änderungen der IP Konfiguration lesen Sie bitte die Anweisungen in den folgenden Kapiteln.

Ein direkter drahtloser Betrieb des Gerätes via Wireless LAN ist nicht möglich.

→ Bitte beachten Sie, dass zum korrekten Funktionieren des Gerätes innerhalb ihrer Telematik Infrastruktur oder mit CT-API LAN Tunnel (s. Abschnitt 11.2.2, Verwendung der CT-API über das LAN*) die korrekte IP Konfiguration (IP Adresse, Subnetz, Gateway) aller Komponenten (Kartenlese-Terminal, Arbeitsplatzrechner, Konnektor,etc.) erforderlich ist.*

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

7.5.1 Kabelverbindungen

Zum Anschluss an das LAN verwenden Sie bitte das mitgelieferte (achtadrige) Ethernet-Kabel oder ein gleichwertiges Patch-Kabel der Kategorie 5. Schließen Sie dieses Kabel zunächst auf der einen Seite an einen verfügbaren Ethernet Port ihres aktivierten LANs an (z.B. Ethernet Hub, Switch oder DSL Router i.d.R. mit mehreren RJ-45 Steckplätzen).

→ Bitte achten Sie auf die Beschriftung Ihres Hubs. Bei manchen Ethernet-Hubs ist der erste LAN Port ein sogenannter UPLINK Port, welcher nicht für die Verwendung mit einem normalen LAN Gerät und einem Standard-Patch-Kabel vorgesehen ist.

Stecken Sie nun das andere Ende des Kabels in den RJ-45 LAN Port an der Rückseite des Gerätes an (Buchse mit der Beschriftung „LAN“). Bei erfolgreicher Kabelverbindung wird nach ca. einer Sekunde eine Zustands-LED direkt am LAN Anschluss permanent aktiviert. Eine zweite LED signalisiert ein- und ausgehende Kommunikation des Terminals ins LAN (z.B. mit einem DHCP Server).

7.5.2 Anschluss eines weiteren Netzwerkgerätes

Das OMNIKEY® 8751 e-Health LAN wird mit einem eingebauten Netzwerk-Hub ausgeliefert. Dies ermöglicht es, in Verkabelungen mit nur einem LAN Anschluss neben dem Terminal noch ein zweites Netzwerkgerät (z.B. Drucker oder Arbeitsplatzstation) anzuschließen.

Ein für diese Verkabelungsart notwendiger Adapter ist nicht im Lieferumfang enthalten. Den Adapter (sog. *Portdoppler für strukturierte Ethernet Verkabelung*) ist als kostenpflichtiges Zubehör erhältlich.

-> Bei der Verwendung des Adapters sind keine weiteren Konfigurationseinstellungen vorzunehmen. Die Portbelegung des Adapters ist frei wählbar.

7.5.3 Automatische Netzwerk-Konfiguration via DHCP

Die Netzwerkschnittstelle des Gerätes erlaubt den Betrieb sowohl an einem 10 Mbit als auch einem 100 Mbit Netzwerk. Bei Anschluss an einen Gigabit Switch (1000 Mbit) erfolgt ein automatischer Verbindungsaufbau mit 100 Mbit.

Die Grundeinstellung des Gerätes setzt ein TCP/IP Netzwerk mit **DHCP Server** (Dynamic Host Configuration Protocol) voraus. Wird ein Netzwerkkabel an der Netzwerkbuchse des Geräts verbunden, so erhält das Gerät automatisch über das DHCP Protokoll eine gültige IP Konfiguration (bestehend aus IP Adresse, Subnetzmaske, Gateway und maximal zwei DNS Server).

→ DHCP Server sind in modernen DSL-Routern standardmäßig enthalten und aktiv.

Das Abziehen des Netzwerkkabels vom Gerät hat eine Dekonfiguration der automatisch konfigurierten Netzwerkschnittstelle zur Folge.

7.5.4 Überprüfung der DHCP Konfiguration

Bei Verwendung eines DHCP Servers ist mit Anschluss des Gerätes am Netzwerk die Netzwerk-Installation abgeschlossen.

Die erfolgreiche Zuweisung einer IP Adresse kann direkt am eingeschalteten Gerät wie folgt überprüft werden:

MENU -> (1) Status -> (1) IP

Mehr Informationen zur Verwendung des Gerätemenüs s. Abschnitt 6 Geräte-Menü.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

Falls im Display keine IP Konfiguration des DHCP Servers angezeigt wird, gehen Sie bitte – je nach angezeigtem Text - wie folgt vor:

Display Anzeige: **„IP: n/a“**

→ *Es existiert keine aktive physikalische Verbindung zum Netzwerk. Bitte überprüfen Sie Stecker, Verkabelung und ihren LAN Anschluss (z.B. Stromversorung des Hubs)*

Display Anzeige: **„IP:<Adresse>“ mit Adresse aus der Range IP: 169.254.*.***

→ *Eine aktive physikalische Verbindung zum Netzwerk besteht. Ein DHCP Server wurde nicht gefunden. Das Gerät hat sich deshalb via AUTO IP selbst eine IP Adresse zugewiesen. Bitte überprüfen Sie ihren DHCP Server (z.B. auf Erreichbarkeit, aktivierte MAC Filter etc.).*

7.5.5 Konfiguration ohne DHCP Server

Ist ein DHCP Server in Ihrem Netzwerk *nicht* verfügbar, kann das Gerät auf zwei Arten konfiguriert werden.

Verwendung zweier Auto-IP Adressen

Das mit einer Auto-IP Adresse versehene Terminal kann mit einem anderen Gerät, welches ebenfalls eine Auto-IP Adresse hat, verbunden werden.

- > Bitte kontaktieren Sie ihren Systemadministrator für weiter Details.

Verwendung eines temporären DHCP Servers

Es gibt unter Linux und MS® Windows verschiedene kostenfreie DHCP Server, welche zur Konfiguration des Terminals installiert und konfiguriert werden können.

- > Bitte kontaktieren Sie ihren Systemadministrator für weiter Details.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

8 Webschnittstelle

8.1 Allgemeines

Das Terminal verfügt über eine HTML-basierende Webschnittstelle, in welcher tiefer gehende Systemeinstellungen abgerufen und geändert werden können. Über die Webschnittstelle erfolgt auch ein Firmware-Upload.

Über die Webschnittstelle können folgende Einstellungen eingesehen werden:

- User-Verwaltung und Änderung der Passwörter
- TCP/IP Konfiguration und Änderung
- Firmware Status und Updates
- Zustand der Smart Card Schnittstellen
- Geräte-Neustart (Warmstart)

Der Aufruf der Webschnittstelle erfolgt über einen normalen Internet-Browser (z.B. Internet Explorer 7 oder Mozilla Firefox 3) mit folgender Browser–URL:

https://<IP Adresse des Gerätes>

Die IP Adresse entspricht dabei der IP-Adresse, welche aktuell dem Gerät zugewiesen ist.

Die aktuelle IP-Adresse des Gerätes kann direkt am eingeschalteten Gerät wie folgt überprüft werden:

MENU -> (1) Status -> (1) IP

→ Falls die Website im Browser nicht erreichbar ist, überprüfen Sie bitte die Proxy-Einstellungen ihres Browsers sowie Ihre Netzwerkkonfiguration.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

8.2 Browser Warnmeldung (Zertifikatefehler)

Bitte ignorieren Sie die Warnmeldungen ihres Browsers, welche sich auf das Zertifikat der aufrufenden Website - also dem Webserver im Terminal - bezieht.

Die Warnmeldung kommt systembedingt zustande, da das Terminal keine echte Internet Website mit fest aus dem Internet erreichbarem DNS Eintrag ist, welcher normalerweise Bestandteil des Zertifikates sein muss. Zudem ist das Zertifikat selbstsigniert.

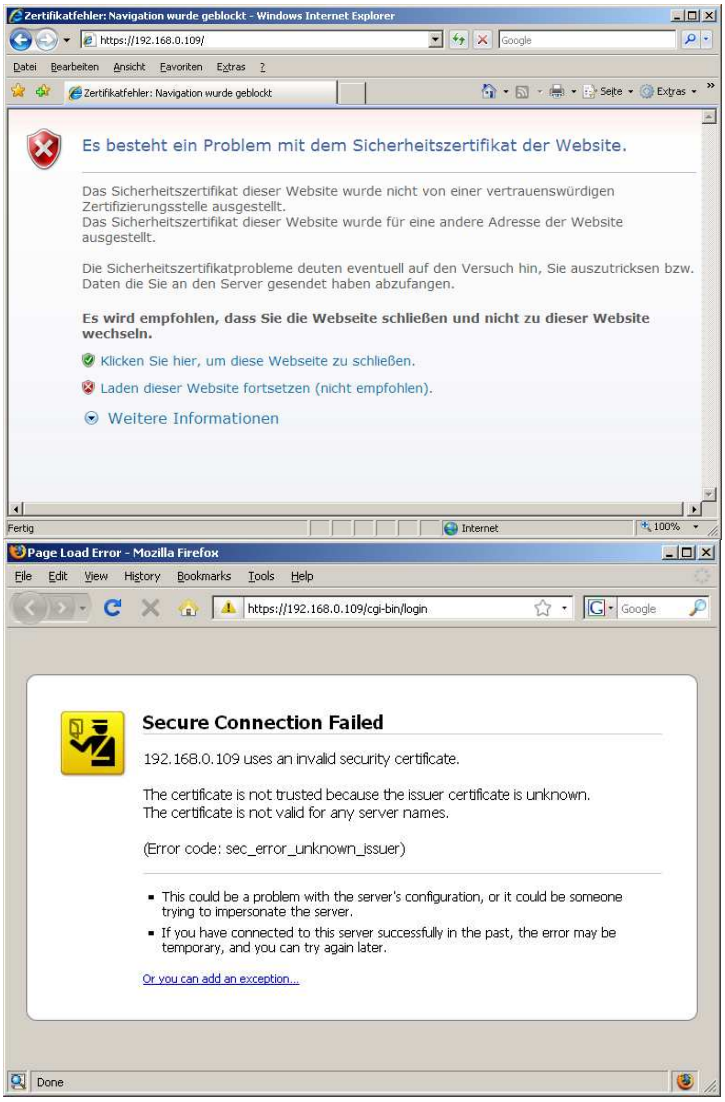
Zertifikatfehler: Navigation wurde geblockt - Windows Internet Explorer
https://192.168.0.109/
Es besteht ein Problem mit dem Sicherheitszertifikat der Website.
Das Sicherheitszertifikat dieser Website wurde nicht von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt.
Das Sicherheitszertifikat dieser Website wurde für eine andere Adresse der Website ausgestellt.
Die Sicherheitszertifikatprobleme deuten eventuell auf den Versuch hin, Sie auszutricksen bzw. Daten die Sie an den Server gesendet haben abzufangen.
Es wird empfohlen, dass Sie die Webseite schließen und nicht zu dieser Website wechseln.
Klicken Sie hier, um diese Webseite zu schließen.
Laden dieser Website fortsetzen (nicht empfohlen).
Weitere Informationen
Page Load Error - Mozilla Firefox
https://192.168.0.109/cgi-bin/login
Secure Connection Failed
192.168.0.109 uses an invalid security certificate.
The certificate is not trusted because the issuer certificate is unknown.
The certificate is not valid for any server names.
(Error code: sec_error_unknown_issuer)
This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.
Or you can add an exception...
Done

Abbildung 14: Zertifikate-Warnmeldung der Webschnittstelle (IE 7 und Firefox)

Bitte klicken Sie im Internet Explorer: *Laden dieser Website fortsetzen...*

Bitte klicken Sie im Mozilla: Or you can add an exception …

8.3 Authentizitätsprüfung der Webschnittstelle

Bei Bedarf kann die Authentizität des Zertifikates auf Basis des folgenden elektronischen Fingerabdrucks von Ihrem Systemadministrator geprüft werden:

```
SHA1 Fingerprint:
cc 62 ce ef 15 0f 25 53 69 88 cd d5 de ff 1d 22 d9 3f 64 17
```


© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

8.4 Login

Nach erfolgreichem Verbindungsaufbau wird die Login-Seite des Terminals im Browser angezeigt.

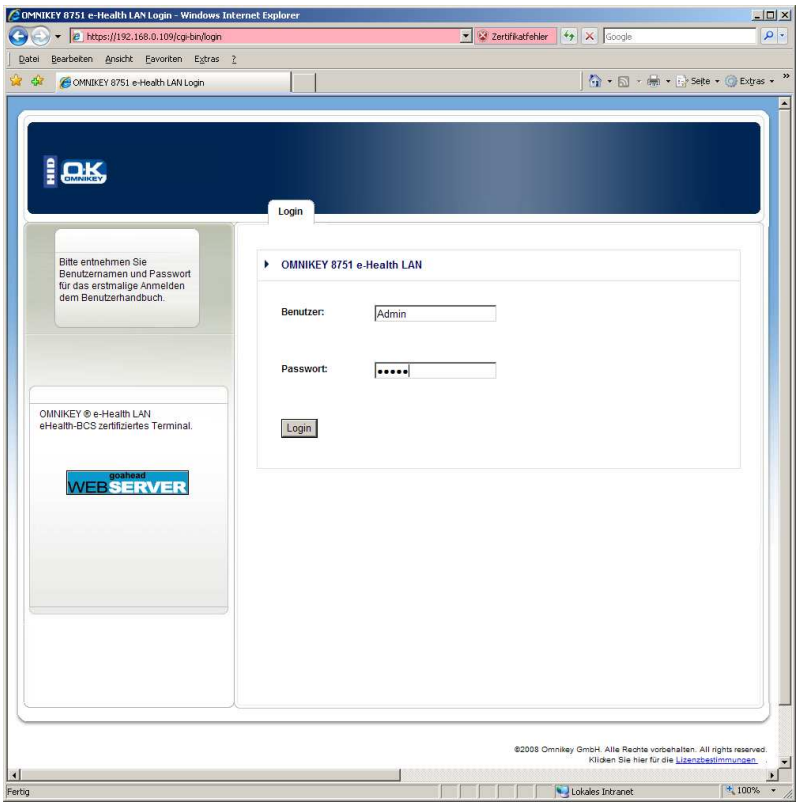

Abbildung 15: Webschnittstelle Login

Die User für den Webzugriff und deren Passwörter im Auslieferungszustand sind:

Administrations-User mit Änderungsrechten

Benutzer: Admin

Passwort: Admin

User mit Leserechten

Benutzer: User

Passwort: User

→ Bitte ändern Sie alle Standard-Passwörter sofort oder spätestens nach erfolgter Konfiguration des Gerätes. Aus Sicherheitsgründen sind die Passwörter nicht rücksetzbar. Bei Verlust der Passwörter ist die Webschnittstelle des Gerätes dauerhaft unbrauchbar.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

8.5 Status Anzeige und Warmstart

Nach erfolgreichem Login erfolgt die Anzeige des Geräte-Status.

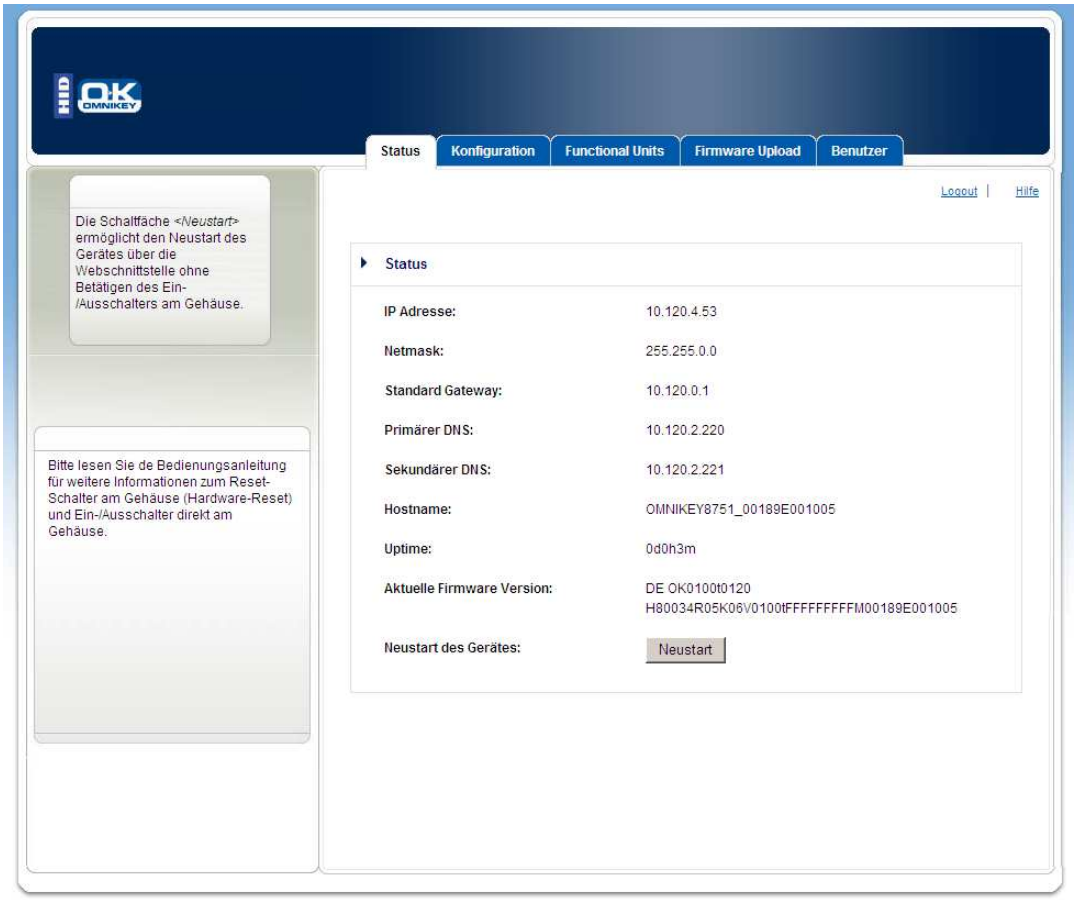
Status
Konfiguration
Functional Units
Firmware Upload
Benutzer
Logout | Hilfe
Die Schaltfäche <Neustart> ermöglicht den Neustart des Gerätes über die Webschnittstelle ohne Betätigen des Ein-/Ausschalters am Gehäuse.
Bitte lesen Sie de Bedienungsanleitung für weitere Informationen zum Reset-Schalter am Gehäuse (Hardware-Reset) und Ein-/Ausschalter direkt am Gehäuse.
Status
IP Adresse: 10.120.4.53
Netmask: 255.255.0.0
Standard Gateway: 10.120.0.1
Primärer DNS: 10.120.2.220
Sekundärer DNS: 10.120.2.221
Hostname: OMNIKEY8751_00189E001005
Uptime: 0d0h3m
Aktuelle Firmware Version: DE OK0100t0120 H80034R05K06V0100tFFFFFFFFFM00189E001005
Neustart des Gerätes: Neustart

Abbildung 16: Status und Neustart Button

Auf der Status-Anzeige stehen wichtige Geräte Details, die z.B. im Supportfalle benötigt werden.

Der Button Neustart erlaubt einen Geräte-Neustart des Gerätes über die Webschnittstelle ohne Betätigen des Ein- / Ausschalters am Gerät oder ziehen des Netzsteckers (sog. Warmstart).

Nach Betätigen der Neustart-Taste ist das Gerät für die Dauer des Neustarts nicht über die Webschnittstelle erreichbar.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

8.6 IP Konfiguration

Über den Reiter Konfiguration können die TCP/IP Einstellungen des Terminals geändert werden.

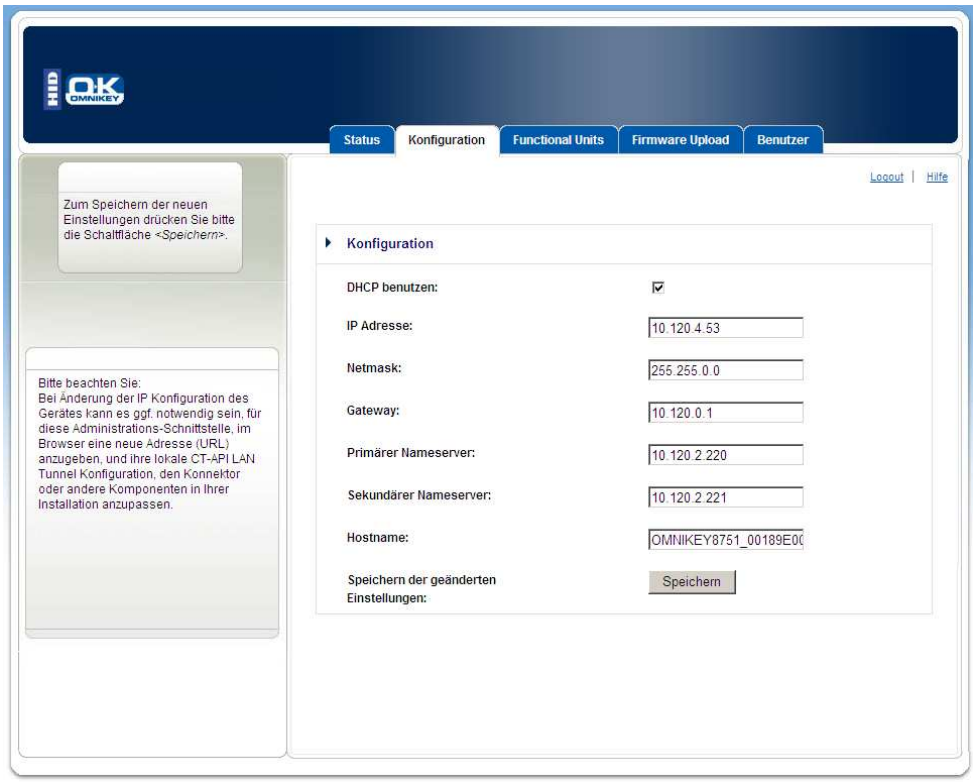

Abbildung 17: Konfigurationsmenü

Die Standardkonfiguration des Gerätes (bei Auslieferung und nach Reset am Gehäuse) ist dabei wie folgt:

- DHCP: Aktiv (Checkbox gesetzt)
- Hostname: Der Hostname wird vor allem zur Konfiguration des Terminals im Konnektor benötigt. Dabei zeigt das Konfigurationsmenü des Konnektors den hier eingestellten Hostnamen an.
  Zur leichteren Identifizierung des Gerätes in einer Mehrgeräte-Umgebung ist der Default-Hostname zusammengesetzt aus dem Gerätenamen plus MAC Adresse des Gerätes (z.B. OMNIKEY8751_00189E001005). Die Mac Adresse befindet sich auch auf einem Aufkleber auf der Gehäuse-Unterseite und kann über das Menü direkt am Gerät abgefragt werden.

Für eine manuelle IP Konfiguration muss DHCP deaktiviert werden (Checkbox entfernen). Die IP Konfiguration muss dabei für das entsprechende LAN gültig sein, in welchem das Gerät später zum Einsatz kommt.

Eine gültige LAN Konfiguration muss mindestens folgende Informationen umfassen:

- IP Adresse
- Subnetz-Maske

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

Folgende Informationen können - abhängig von Ihrer Netzwerkkonfiguration (insbesondere in größeren Installationen) - ebenfalls erforderlich sein:

- Gateway
- Primärer und sekundärer Nameserver

Zum Speichern von Änderungen drücken Sie bitte die Schaltfläche <Speichern>.

Eine manuell konfigurierte Netzwerkeinstellung bleibt auch bei einem Neustart oder bei Trennung vom Stromnetz erhalten.

→ Wird eine manuell eingestellte IP-Konfiguration aktiv, ist das Gerät und damit die Webschnittstelle nur noch von Geräten mit passender LAN Konfiguration erreichbar und konfigurierbar.

Die Webschnittstelle kann nur noch unter der neuen IP Adresse erreicht werden.

Ein Konnektor muss ggf. neu mit dem Gerät verbunden werden.

Bei einer Fehlkonfiguration kann durch ein Hardware-Reset (s. Abschnitt 9) die IP-Konfiguration des Auslieferungszustandes einfach wiederhergestellt werden.

8.7 Functional Units

Der Reiter Functional Units stellt den aktuellen Zustand der einzelnen Gerätekomponenten dar.

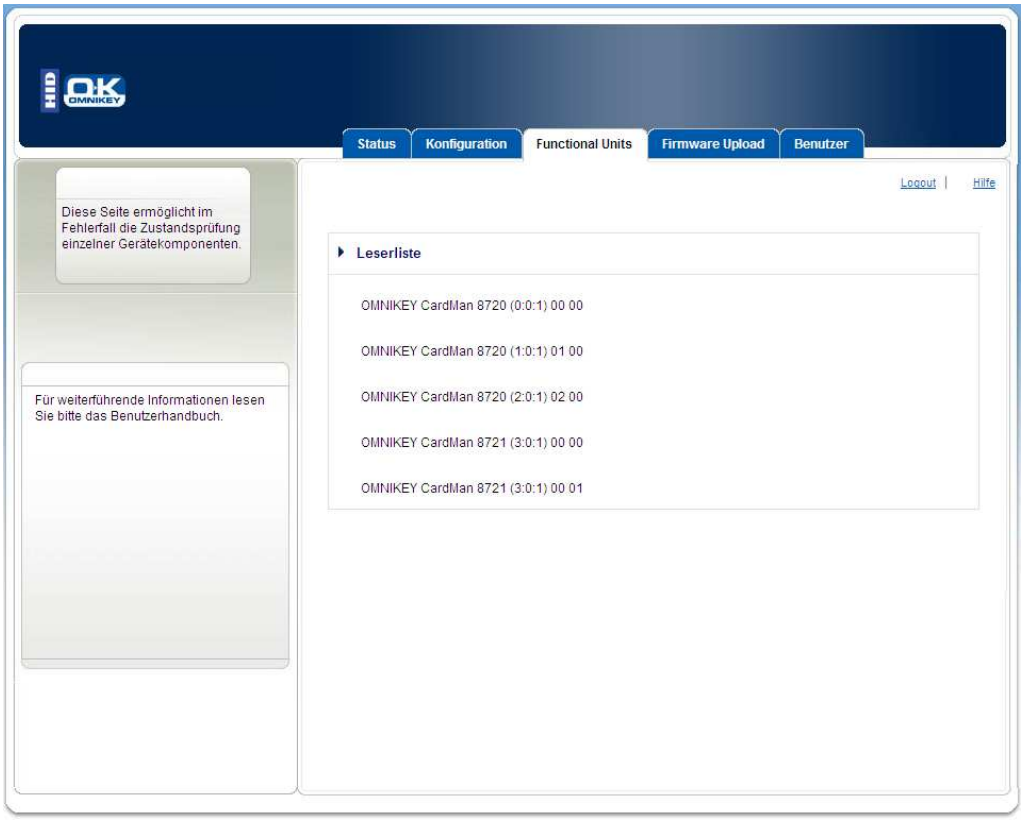
Status
Konfiguration
Functional Units
Firmware Upload
Benutzer
Logout | Hilfe
Diese Seite ermöglicht im Fehlerfall die Zustandsprüfung einzelner Gerätekomponenten.
Für weiterführende Informationen lesen Sie bitte das Benutzerhandbuch.
Leserliste
OMNIKEY CardMan 8720 (0:0:1) 00 00
OMNIKEY CardMan 8720 (1:0:1) 01 00
OMNIKEY CardMan 8720 (2:0:1) 02 00
OMNIKEY CardMan 8721 (3:0:1) 00 00
OMNIKEY CardMan 8721 (3:0:1) 00 01

Abbildung 18: Functional Units

Diese Anzeige ist aktuell nur im Fehlerfall relevant. Mit ihr kann ein ggf. auftretender Fehler am Gerät genauer identifiziert werden.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

8.8 Firmware Upload

Über den Reiter Firmware Upload ist die aktuell installierte Firmware-Version des Terminals ersichtlich. Zudem kann hier eine neue Firmware eingespielt werden.

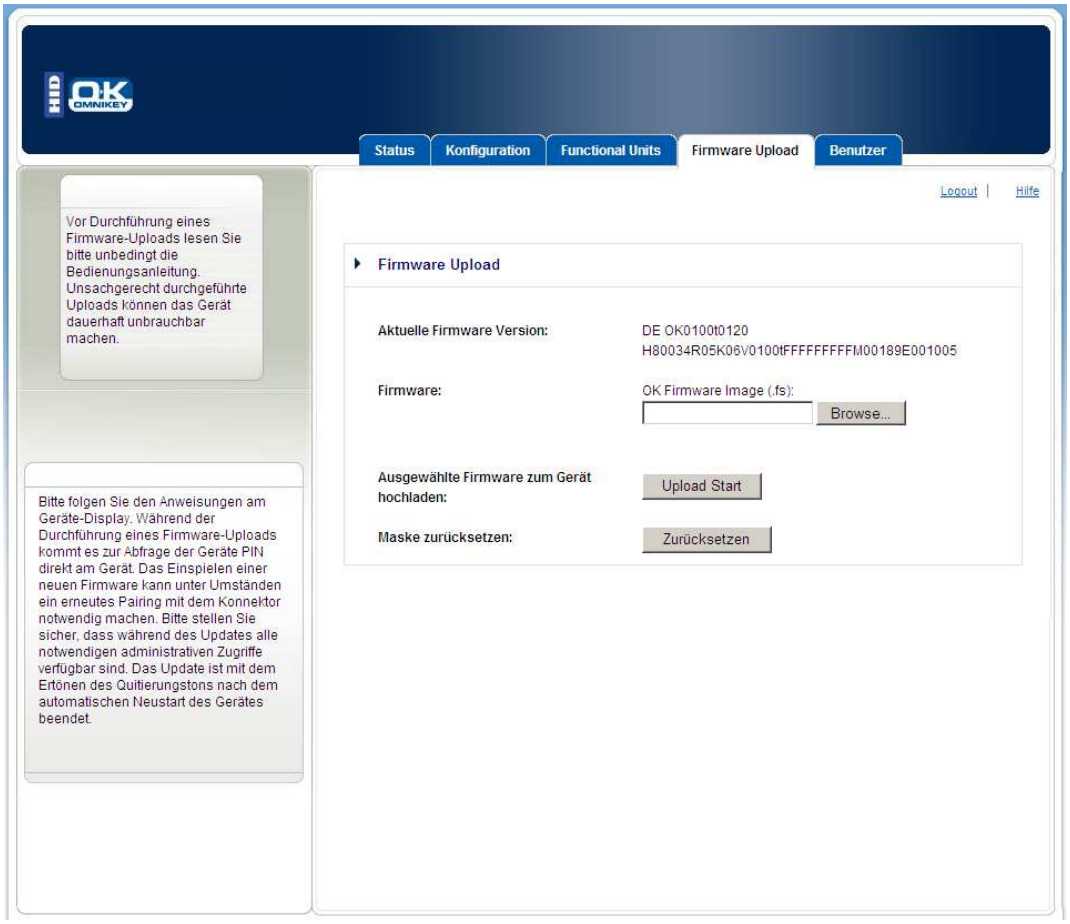
Status
Konfiguration
Functional Units
Firmware Upload
Benutzer
Logout | Hilfe
Vor Durchführung eines Firmware-Uploads lesen Sie bitte unbedingt die Bedienungsanleitung. Unsachgerecht durchgeführte Uploads können das Gerät dauerhaft unbrauchbar machen.
Firmware Upload
Aktuelle Firmware Version:
DE OK0100t0120
H80034R05K06V0100tFFFFFFFFFM00189E001005
Firmware:
OK Firmware Image (.fs):
Browse...
Ausgewählte Firmware zum Gerät hochladen:
Upload Start
Maske zurücksetzen:
Zurücksetzen
Bitte folgen Sie den Anweisungen am Geräte-Display. Während der Durchführung eines Firmware-Uploads kommt es zur Abfrage der Geräte PIN direkt am Gerät. Das Einspielen einer neuen Firmware kann unter Umständen ein erneutes Pairing mit dem Konnektor notwendig machen. Bitte stellen Sie sicher, dass während des Updates alle notwendigen administrativen Zugriffe verfügbar sind. Das Update ist mit dem Ertönen des Quitierungstons nach dem automatischen Neustart des Gerätes beendet.

Abbildung 19: Reiter Firmware Upload

Details zum Upload einer neuen Firmware finden Sie in Abschnitt 10 Upgrade von Firmware.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

8.9 Passwörter ändern

Über den Reiter Benutzer können die Passwörter für die Benutzer geändert werden.

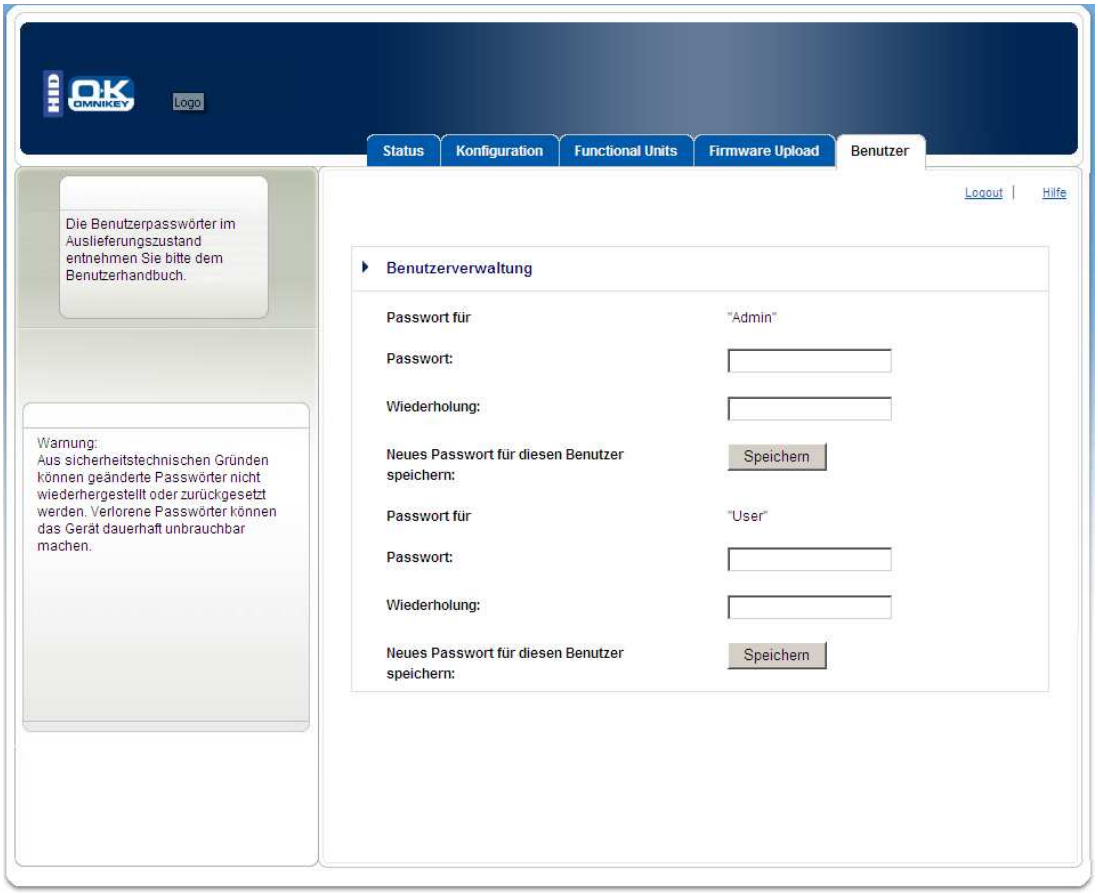

Abbildung 20: Benutzerpasswörter ändern

Im Auslieferungszustand sind die Passwörter wie folgt eingestellt:

Administrations-User mit Änderungsrechten

Benutzer: Admin

Passwort: Admin

User mit Leserechten

Benutzer: User

Passwort: User

→ Bitte ändern Sie alle Standard-Passwörter sofort oder spätestens nach erfolgter Konfiguration des Gerätes. Aus Sicherheitsgründen sind die Passwörter nicht rücksetzbar. Bei Verlust der Passwörter ist die Webschnittstelle des Gerätes nicht mehr brauchbar.

→ Eine Änderung der Benutzernamen „Admin“ und „User“ ist nicht möglich.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

9 Hardware-Reset

Der Reset-Schalter des Terminals befindet sich auf der Gehäuse-Rückseite (s. Abbildung 5: Geräte-Elemente hinten) und kann mit einem spitzen Stift (z.B. einer Büroklammer) ausgelöst werden.

Für ein Reset muss der Schalter für ca. 5 Sekunden gedrückt werden. Nach einem erfolgreichen Reset durchläuft das Gerät für ca. 30 Sekunden einen Selbsttest mit abschließendem doppelten Quittungston.

→ *Mit dem Reset werden die LAN Einstellungen des Gerätes in den Auslieferungszustand zurückversetzt. Alle manuell getätigten Einstellungen (IP Adresse, Subnetz Maske, Gateway, DNS Server und Hostname) gehen dabei verloren.*

Folgende Einstellungen werden bei einem Hardware-Reset zurückgesetzt:

Standardwerte für die Netzwerkkonfiguration:

- DHCP ist aktiv
- IP Adresse und Netzmaske undefiniert oder mit Werten aus einem nicht routebaren Adressbereich [RFC1918] vorbelegt.
- Terminal Name (Default Hostname)
- DNS Server
- Gateway Adresse

Standardwerte für die V.24 (serielle) Schnittstelle

- Übertragungsgeschwindigkeit = 9.600 Baud
- Namen für die FU's entsprechend der hersteller- oder fachspezifischen Sicht

Dieses Verhalten kann sich bei zukünftigen Firmware-Versionen auf Grund von Sicherheitsbestimmungen ändern.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

10 Upgrade von Firmware

10.1 Allgemeines

Das Gerät verfügt über eine Upgrade-Funktion für Firmware. Diese stellt den reibungslosen Übergang vom eHealth BCS Szenario auf das eHealth Szenario sicher. Für ein Upgrade darf nur Originalfirmware des Herstellers benutzt werden, die durch die "gematik" zugelassen wurde. Der Hersteller garantiert dies durch eine in das Upgrade eingebrachte Signatur. Nicht oder falsch signierte Firmware wird durch das Gerät abgewiesen. Ein Upgrade ist nur mit der gleichen oder einer höheren Firmware-Version möglich. Der Versuch auf eine ältere Firmware-Version einzuspielen, wird durch das Gerät abgewiesen.

Zur Finalisierung eines Upgrade wird der Betreiber zur Eingabe der Geräte-PIN aufgefordert. Ohne diese PIN-Eingabe kann das Upgrade nicht zu Ende geführt werden.

Vor einem Upgrade auf das eHealth Szenario mit Betrieb des Gerätes am Konnektor, ist der Betreiber verpflichtet zu kontrollieren, ob das Gerät (die Firmware) für den Betrieb in seiner speziellen Signaturanwendungskomponente (SAK) bestätigt ist. Dazu ist die Liste der bestätigten Komponenten bei der Bundesnetzagentur (BNetzA) einzusehen.

http://www.bundesnetzagentur.de →Sachgebiete → Elektronische Signatur

Nur wenn diese Bestätigung vorliegt, darf das Upgrade finalisiert werden.

10.2 Quelle für neue Firmware

Eine neue verfügbare Firmware wird im Normalfall über folgende Website zum Download zur Verfügung gestellt: http://www.hidglobal.com/8751de

Alternativ kann eine neue Firmware über den Fachhandel oder der gematik bezogen werden.

Bitte beachten Sie unbedingt die mit der neuen Firmware veröffentlichten Dokumentationen, Kompatibilitäts- und Lizenzierungshinweise.

10.3 Sicherheitshinweise

Bitte beachten Sie unbedingt die folgenden Sicherheitshinweise vor dem Durchführen eines Firmware Updates.

Ausführungen zum *Konnektor* gelten nur, falls sich dieser in Ihrer Telematik-Infrastruktur bereits im Einsatz befindet (z.B. im Rahmen einer Testinstallation).

- Kein Firmware Update ohne Grund („Never change a running system“)

Bitte führen Sie ein Firmware Update nur durch, wenn es dazu einen konkreten Anlass gibt (z.B. vom Hersteller oder der gematik empfohlen bei Übergang vom eHealth BCS auf das eHealth Szenario).

- Durchführung nur durch Ihren Systemadministrator

Das Firmware Update sollte nur von geschultem Personal durchgeführt werden, welches mit Ihrer Infrastruktur vertraut ist.

- Kein Update während oder kurz vor den Nutzungszeiten (z.B. Praxis-Öffnungszeiten)

Führen Sie kein Firmware Update „mal zwischendurch“ aus. Eine bestehende Praxis- oder Telematik-Infrastruktur kann aus mehreren, komplex vernetzten Komponenten bestehen. Daher besteht nach einem Eingriff das Restrisiko eines Fehlers im Zusammenspiel der Komponenten.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

- Voller physikalischer und logischer Geräte-Zugriff

Durch ein Firmware Update besteht die Möglichkeit, dass e-Health Komponenten erneut konfiguriert werden müssen (z.B. neues Einrichten und Konfigurieren des Lesers in Ihrer PVS Software, Pairing zwischen Konnektor und Terminal etc.). Bitte stellen Sie vor dem Update sicher, dass Sie entsprechenden physikalischen und logischen Zugriff auf alle Infrastruktur-Komponenten haben (z.B. Admin-Passwörter für Rechner- und Serversysteme sowie Schlüssel für EDV-Schränke zum Durchführen eines Geräte-Kaltstarts).

- Konfiguration notieren

Bitte notieren Sie sich **vor** dem Einspielen des Updates die Konfiguration des Gerätes. Bei Verwendung der seriellen Schnittstelle notieren Sie insbesondere bitte die am Gerät eingestellte Baud-Rate, bei Verwendung der LAN Schnittstelle insbesondere die Netzwerkkonfiguration bei fest konfigurierter IP Adresse. Notieren Sie ggf. alle weiteren Einstellungen Ihrer lokalen Software (z.B. bisher verwendeter COM Port oder CT-API Einstellung).

- Firmware Versionen notieren und prüfen

Bitte prüfen und notieren Sie vor dem Einspielen der Firmware die **aktuelle** Versionsnummer sowie die neue Versionsnummer der Firmware. Prüfen Sie, ob die neue Firmware für Gerät und Konnektor passt bzw. empfohlen ist (s. auch Abschnitt 10.1).

- Konnektor ausschalten oder vom Netz nehmen

Um jegliche Störung des Updates durch den Konnektor auszuschließen, schalten Sie den Konnektor bitte während eines Terminal-Updates aus oder nehmen den Konnektor vom Netzwerk.

- Karten entfernen und Knöpfe nur auf Anfrage drücken

Bitte entfernen Sie vor einem Update alle Chipkarten aus dem Gerät, welche frei entfernbar sind. Mit einem Siegel gesicherte Karten verbleiben im Gerät. Bitte drücken Sie während des Updates Knöpfe am Gerät nur auf Anfrage.

- Stromversorgung sicherstellen

Stellen Sie sicher, dass während des gesamten Updates die Stromversorgung zum Gerät nicht unterbrochen wird. Schalten Sie das Gerät während des Vorgangs nur dann aus, wenn Sie zum Neustart aufgefordert werden. Eine Unterbrechung während des Updates kann das Gerät dauerhaft unbrauchbar machen.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

10.4 Durchführung des Updates

Bitte greifen Sie mit einem Browser (z.B. Internet Exporer oder Mozilla Firefox) wie unter Abschnitt 8 beschrieben auf die Webschnittstelle des Gerätes zu und loggen sich als *Administrator* ein.

Wechseln Sie auf den Reiter Firmware Upload.

Wählen Sie im Feld *Firmware* die Firmware-Datei aus, welche auf das Terminal neu eingespielt werden soll, und drücken Sie dann die Schaltfläche <Upload Start>.

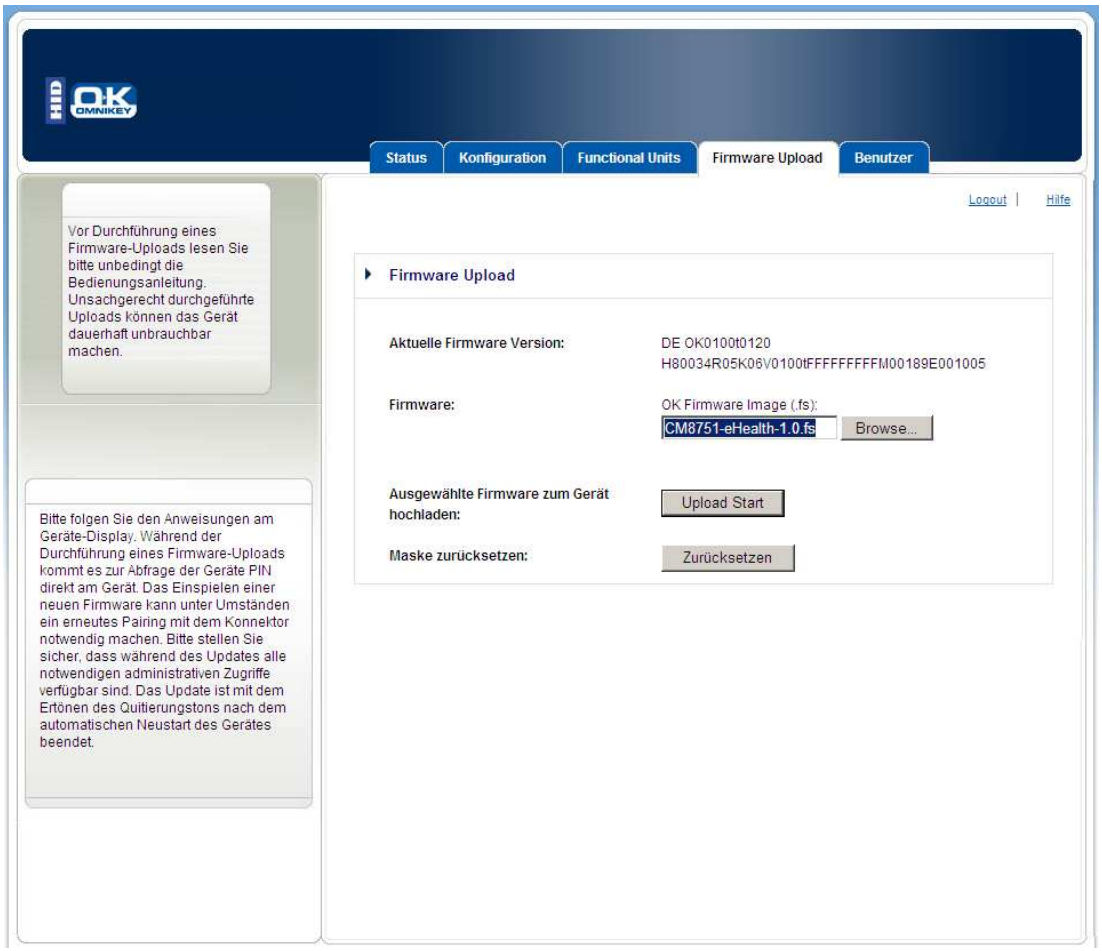
Status
Konfiguration
Functional Units
Firmware Upload
Benutzer
Logout | Hilfe
Vor Durchführung eines Firmware-Uploads lesen Sie bitte unbedingt die Bedienungsanleitung. Unsachgerecht durchgeführte Uploads können das Gerät dauerhaft unbrauchbar machen.
Firmware Upload
Aktuelle Firmware Version:
DE OK0100t0120
H80034R05K06V0100tFFFFFFFFFM00189E001005
Firmware:
OK Firmware Image (.fs):
CM8751-eHealth-1.0.fs
Browse...
Ausgewählte Firmware zum Gerät hochladen:
Upload Start
Maske zurücksetzen:
Zurücksetzen
Bitte folgen Sie den Anweisungen am Geräte-Display. Während der Durchführung eines Firmware-Uploads kommt es zur Abfrage der Geräte PIN direkt am Gerät. Das Einspielen einer neuen Firmware kann unter Umständen ein erneutes Pairing mit dem Konnektor notwendig machen. Bitte stellen Sie sicher, dass während des Updates alle notwendigen administrativen Zugriffe verfügbar sind. Das Update ist mit dem Ertönen des Quitierungstons nach dem automatischen Neustart des Gerätes beendet.

Abbildung 21: Firmware Upload

Die Übertragung der neuen Firmware kann einige Minuten dauern.

Nach erfolgreicher Übertragung der Firmware erscheint die Neustart-Seite im Browser.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

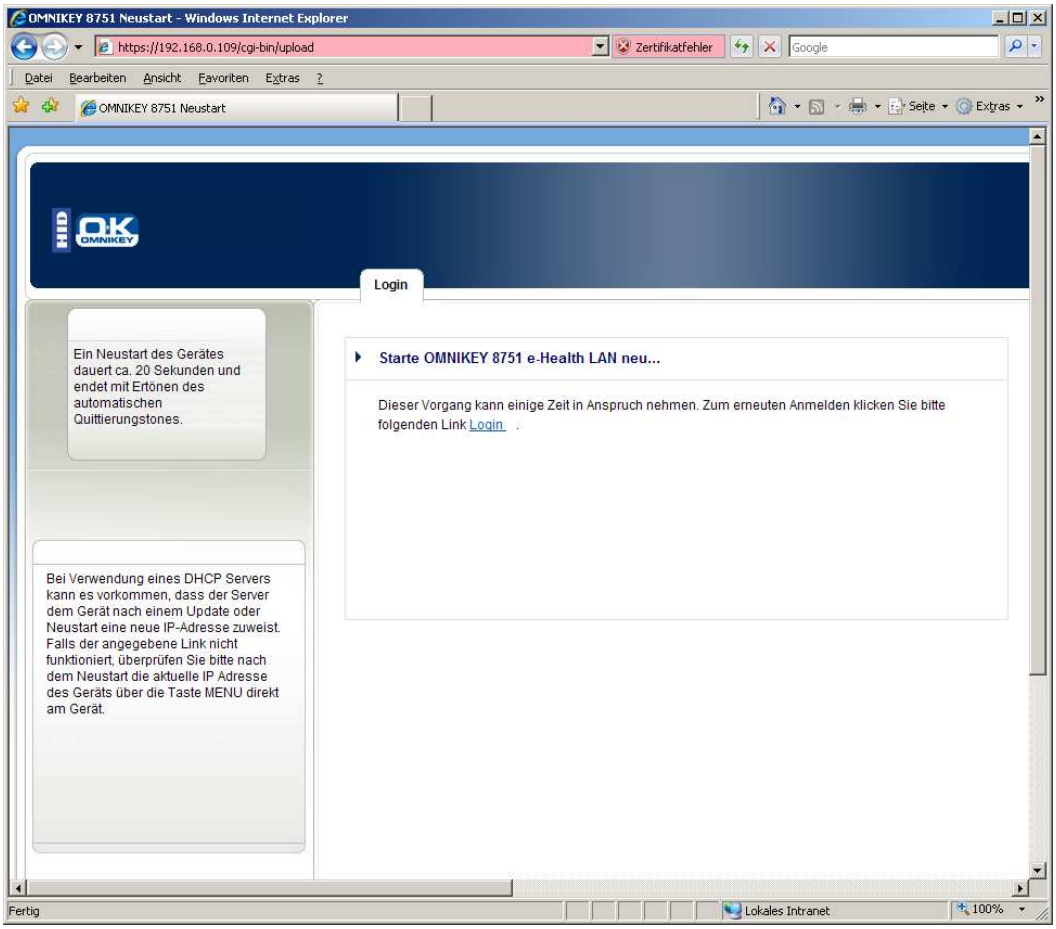
OMNIKEY 8751 Neustart - Windows Internet Explorer
https://192.168.0.109/cgi-bin/upload
Zertifikatfehler
Google
Datei Bearbeiten Ansicht Favoriten Extras ?
OMNIKEY 8751 Neustart
Seite
Extras
Login
Ein Neustart des Gerätes dauert ca. 20 Sekunden und endet mit Ertönen des automatischen Quittierungstones.
Starte OMNIKEY 8751 e-Health LAN neu...
Dieser Vorgang kann einige Zeit in Anspruch nehmen. Zum erneuten Anmelden klicken Sie bitte folgenden Link Login .
Bei Verwendung eines DHCP Servers kann es vorkommen, dass der Server dem Gerät nach einem Update oder Neustart eine neue IP-Adresse zuweist. Falls der angegebene Link nicht funktioniert, überprüfen Sie bitte nach dem Neustart die aktuelle IP Adresse des Geräts über die Taste MENU direkt am Gerät.
Fertig
Lokales Intranet
100%

Abbildung 22: Neustart-Seite

Nach dem Neustart ist aus Sicherheitsgründen die Eingabe der Geräte-PIN direkt am Gerät erforderlich. Die Eingabeaufforderung erfolgt sowohl akustisch als auch am Display.

Erst nach erfolgreicher Geräte-PIN Eingabe erfolgt die Programmierung der Firmware mit automatischem Neustart.

Mit Ertönen des automatischen Quittungstones nach dem Neustart ist die Programmierung abgeschlossen.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

11 BCS Funktion

BCS steht für BASIC COMMAND SET in Anlehnung an den Basic Command Set eines KVK Lesegerätes.

Das OMNIKEY® 8751 e-Health LAN ist mit einem seriellen und einem LAN Anschluss ausgestattet, welche den Betrieb des Terminals als BCS fähiges Terminal in verschiedenen Konfigurationen erlauben. Die verschiedenen Konfigurationsmöglichkeiten im BCS Betrieb sind in den folgenden Abschnitten beschrieben.

11.1 Direkte Verwendung der seriellen Schnittstelle

Erlaubt die im Einsatz befindliche Software-Anwendung (z.B. Ihre Praxis-Verwaltungssoftware PVS) das direkte Ansprechen eines Terminals über die serielle Schnittstelle (ohne CT-API.DLL), so muss das Terminal lediglich mit dem PC verbunden werden, und in der Software die korrekte serielle Schnittstelle (COM Schnittstelle) konfiguriert werden.

-> Sofern an der gleichen COM Schnittstelle bereits ein Gerät betrieben wurde, prüfen Sie bitte zunächst, ob das OMNIKEY 8751 ohne Änderung der Konfiguration direkt weiter betrieben werden kann. Ggf. ist am Gerät nur eine andere Baud Rate (s. Abschnitt 6.3 Änderung der Baudrate) einzustellen.

11.2 Verwendung der CT-API

Für das Gerät ist zusätzlich ein CT-API Installationsprogramm auf der mitgelieferten CD-ROM im Ordner CT-API verfügbar. Dieses Programm läuft nur unter *MS Windows® XP und Vista*. Es installiert optional zwei unterschiedliche CT-API Versionen zur Verwendung durch ihre Software, sofern diese Software zur Verwendung einer CT-API DLL Datei ausgelegt ist. In diesem Fall ist normalerweise der genaue Pfad zur installierten DLL Datei zu konfigurieren.

Details zur CT-API Installation und den BCS Funktionen finden Sie im folgenden Abschnitt sowie auf der CD-ROM.

-> Ggf. verfügbare Updates der CT-API finden Sie unter http://www.hidglobal.com/8751de .

11.2.1 Verwendung der CT-API über die serielle Schnittstelle

Die CT-API Installation kopiert optional die Datei **ct8751com.dll** (Default-Pfad "c:\Programme\OMNIKEY\8751 e-Health"), welche zum Berieb des Terminals an der seriellen COM Schnittstelle vorgesehen ist. Dazu muss ihre Software auf diese CT-API konfiguriert werden.

Sofern Ihre Software bereits mit alternativen CT-API DLL Dateien ausgestattet ist, welche zur Verwendung mit der seriellen Schnittstelle konfiguriert sind, so ist unter Umständen ein Betrieb mit der bereits installierten CT-API möglich - ohne die Notwendigkeit einer weiteren Konfigurationsänderung.

-> Sofern an der gleichen Schnittstelle bereits ein Gerät mit CT-API betrieben wurde, prüfen Sie bitte zunächst, ob das OMNIKEY 8751 ohne Änderung der Konfiguration direkt weiter betrieben werden kann. Ggf. ist am Gerät nur eine andere Baud Rate (s. Abschnitt 6.3 Änderung der Baudrate) einzustellen.

11.2.2 Verwendung der CT-API über das LAN (CT-API LAN Tunnel)

Die CT-API Installation kopiert optional die Datei **ct8751.dll** (Default-Pfad "c:\Programme\OMNIKEY\8751 e-Health"), welche das Ansprechen des Terminals über das Lokale Netzwerk (LAN) erlaubt. Das Ansprechen des im LAN angeschlossenen Terminals wird auch als sogenannter *CT-API LAN Tunnel* bezeichnet.

Details zur CT-API Installation finden Sie auf der CD-ROM.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

-> Ein über das LAN mittels CT-API LAN Tunnel verwendetes BCS Terminal benötigt keinen Anschluss über die serielle Schnittstelle mehr.

11.3 Mehrbenutzerbetrieb im LAN

Grundsätzlich kann das Gerät über den LAN Anschluss von mehreren Arbeitsplatzstationen angesprochen werden. Dazu ist keine besondere Konfiguration des Gerätes erforderlich. Es muss lediglich die CT-API für das LAN auf allen Stationen korrekt installiert sein.

-> Das Gerät bleibt solange für alle anderen Arbeitsplätze gesperrt, bis der aktuelle Vorgang einer Arbeitsplatzstation abgeschlossen ist.

11.4 Dualbetrieb Seriell und LAN

Ein Dualbetrieb des Gerätes über serielle Schnittstelle und LAN ist grundsätzlich möglich.

Das Gerät muss dabei gleichzeitig über LAN als auch über die serielle Schnittstelle angeschlossen sein (z.B. seriell an einen direkt am Gerät stehenden Rechner sowie über LAN an einer entfernt stehenden Arbeitsplatzstation).

-> Sobald das Gerät erstmalig über die serielle Schnittstelle angesprochen wurde, ist eine Ansprache über LAN erst nach einem Neustart des Gerätes möglich.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

12 SICCT Funktion

12.1 Service Discovery

Der OMNIKEY® 8751 e-Health LAN kann über das im SICCT Standard v1.20 definierte Service Discovery Protokoll automatisiert aufgefunden werden, indem entsprechende TCP/UDP Broadcast's an Port 4742 gerichtet werden. Voraussetzung ist lediglich die erfolgreiche Konfiguration der Netzwerkschnittstelle des Gerätes und die Erreichbarkeit desselben im jeweiligen Netzwerk.

Es wird erwartet, dass die Service Discoveryanfrage mittels gerichtetem Broadcast gestellt wird. Das bedeutet, dass sich die Broadcastadresse aus IP Adresse des Subnetzes und der Subnetzmaske errechnet. Die „lokale" Broadcastadresse 255.255.255.255 wird nicht verwendet.

Nach einer korrekten Installation Ihrer Telematik-Komponenten sollte das Terminal problemlos von dem von Ihnen eingesetzten Konnektor gefunden werden.

12.2 Kommando-Interpreter

Der SICCT Kommandointerpreter des OMNIKEY® 8751 e-Health LAN erwartet gemäß dem Standard Verbindungen auf TCP/IP 4742.

Die Unterstützung von Transportsicherungsprotokollen/ -mechanismen wird entsprechend im Dienstbeschreibungspaket des Service Discovery Protokolls angezeigt.

Es werden folgende Kommandos entsprechend dem SICCT Standard v1.20 implementiert sein:

- FU und Karten Events
- RESET CT
- REQUEST ICC
  - ATR Data Object
  - Historical Byte Data Object
- EJECT ICC
- GET STATUS
  - FU Data Object
- OUTPUT
- ISO 7816 Kommandos

Die genaue Beschreibung und den Aufbau der Kommandos, sowie der Datenobjekte entnehmen Sie dem SICCT Standard Dokument. Der SICCT Standard ist unter Schirmherrschaft von TELETRUST Deutschland entwickelt worden und kann auf den TELETRUST Internetseiten unter:

http://www.teletrust.de → Publikationen → Fachbeiträge → Spezifikationen

eingesehen werden.

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.

13 Konformitätserklärung

CE Declaration of Conformity

The shipped version of this device complies with the requirements of the directives 89/336/EWG, 73/23/EWG and 1999/5/EG.

EC Declaration of Conformity
Page 1 of 1

Manufacturer:	OMNIKEY GmbH
Address:	Am Klingenweg 6a 605396 Walluf Germany
Product Description:	OMNIKEY 8751

The products described above in the form as delivered is in conformity with the following European Directives:

1999/5/EG	Directive of European Parliament and of the council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

Conformity of the directives is assured through the application of the following standards:

Reference Number	*Edition*
EN 300330-2	V1.1.1
EN 300330-1	V1.1.1
ETSI EN 301489-1	V1.6.1
ETSI EN 301489-3	V1.4.1
EN60950-1	2001
Amendment A11 to EN60950-1	2004

Walluf, 10/12/2008	Uwe Schnabel, Director R&D	
Location, Date	Name, Function	Signature

This declaration certifies the conformity of the specified standards but contains no assurance of properties.

© 2008 OMNIKEY GmbH. All rights reserved. Alle rechte vorbehalten.

Ihre Installationsnotizen

© 2008 OMNIKEY GmbH All rights reserved. Alle Rechte vorbehalten.